Regarding the (N, k)-threshold schemes realization based on modular arithmetic algorithms

OXANA MEZENTSEVA AND ALEKSANDR ALEKSEEV

Abstract

The paper deals with the aspects of distributed data representation model, based on (N, k)-threshold schemes and modular arithmetic, namely, the system of residual classes, what leads to a high degree of parallelism and, as follows, high execution speed of the proposed model. Also specified are some possible hardware solutions, the efficiency calculation results.

Mathematics Subject Classification 2000: 65Y05, 65Y10
General Terms: modular arithmetic, system of residual classes, parallelism
Additional Key Words and Phrases: threshold schemes, Galois fields, NM6403 processor

Recently, in the face of rapid network technologies development, it has become increasingly important to develop effective ways to protect information transmitted over the network. One of the most used and effective methods is to distribute Certification Center's functions among all members of the network through a threshold scheme [2]. Protocols using in such systems have two important characteristics:

- verifiability of distributed computations (ability to verify information from each node participating in the distributed calculation);
- interchangeability of distributed computing agents (insensibility to loosing the link with one or more participants).

As can be seen from the mentioned characteristics, systems operating on the basis of threshold schemes are of interest not only in information security challenges, but also in the field of distributed computing. One possible application of the threshold schemes in a distributed data storage system is shown in [3]. This report briefly describes the application of modular arithmetic and parallel computing for improving a performance rate of the systems, operating on the basis of threshold schemes.

It is advisable to use Shamir's secret sharing scheme as a threshold scheme. A.Shamir proposes a method of dividing some data D (e.g., the safe combination) into pieces $D_1,...,D_n$ in such a way that knowledge of any k or more D_i pieces makes D easily computable and knowledge of any $k-1$ or fewer D_i pieces leaves D

completely undetermined (in the sense that all its possible values are equally likely). This scheme is called (k,n) threshold scheme.

Consider Galois field $P = GF(N)$. Any bit-sequence for $N = 2n$ can be represented as a sequence of n-bit P-elements arrays. Consider the k-dimensional space of vectors L over the field P. Now, any sequence can be thought of as a sequence of vectors from L [3]. The fundamental scheme of proposed in [3] algorithm is shown in Figure 1.

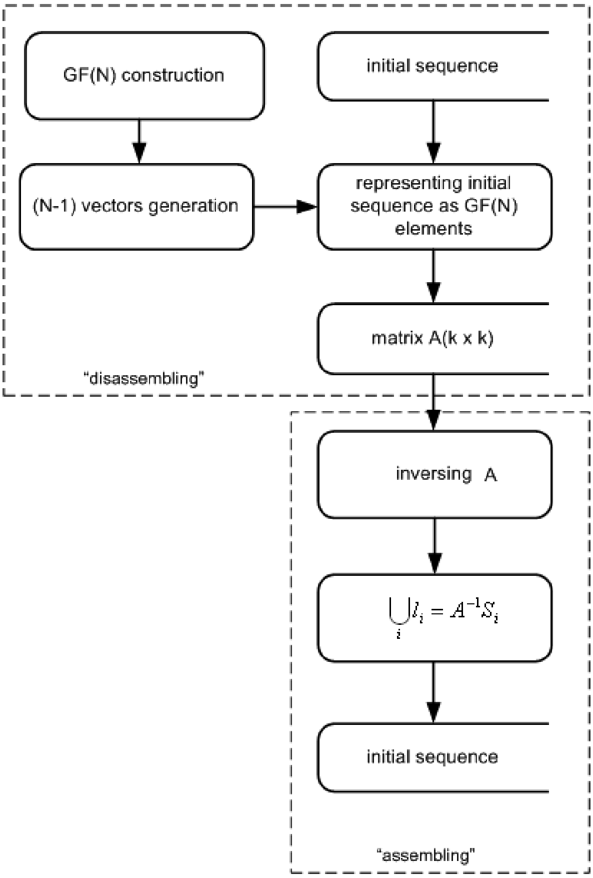

Fig. 1. “Assembling-disassembling” algorithm scheme.

It is clear, that certain operations (field *GF(N)* construction, vector sets generation, disassembling of the initial sequence, inversing matrix A) are performed only once, and while using vector processor (as shown below), the number of operations performed at the stage of disassembling can be significantly reduced, the practical utility of this approach is questionable. The most time-consuming part of the algorithm is the $A^{-1}S_i$, where $S_i = Al_{\mathrm{i}}$ operation, which consists, as shown in [3], of k^2 addition and multiplication operations over Galois field, which in turn is k^2 of normal adding and multiplying and $2k^2$ of % operations (residue of division by N).

As can be seen, moving from calculations in Galois field to the normal operations is associated with a significant increase in the overall algorithm complexity, and, given that the computing of % operation for SISD processors is about four times computing a single multiplication operation, it is proposed to refrain from moving and perform all the necessary calculations in Galois field.

It is proposed to use a mathematical apparatus of residual classes system, which is able of handling each part of given sequence independently on different processors or different parts of one processor in case of SIMD architecture. In this case, computing scheme takes the form presented in Figure 2.

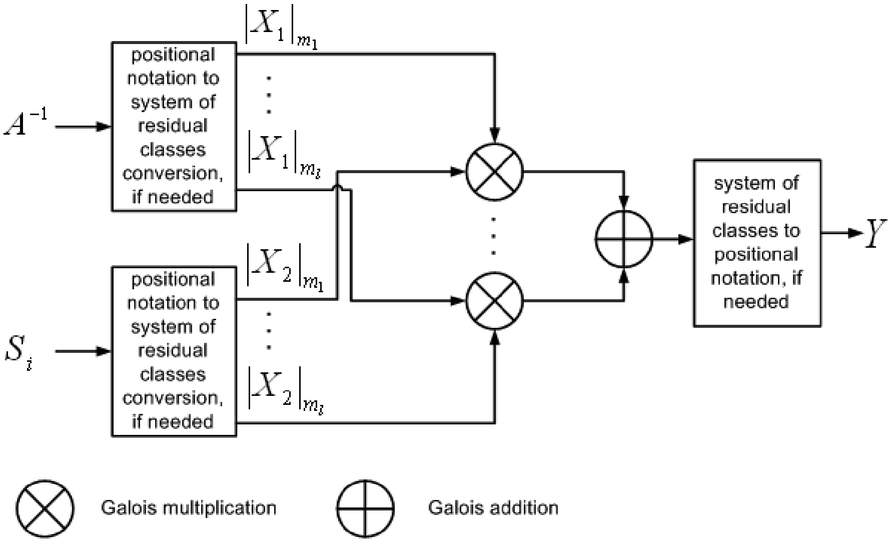
A^{-1}
positional notation to system of residual classes conversion, if needed
$|X_1|_{m_1}$
$|X_1|_{m_l}$
S_i
positional notation to system of residual classes conversion, if needed
$|X_2|_{m_1}$
$|X_2|_{m_l}$
system of residual classes to positional notation, if needed
Y
Galois multiplication
Galois addition

Fig. 2. $A^{-1}S_i$ computation using the system of residual classes.

It is proposed to use the adder without LUT-tables and multiplier based on the power calculus (Galois multiplier) which schemes are shown in Figures 4 and 5, respectively [1].

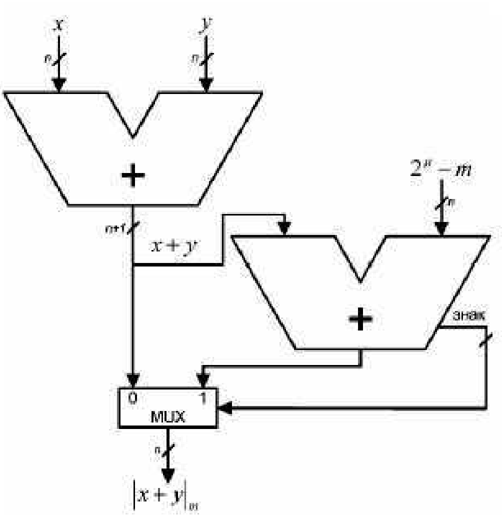

Fig. 3. Adder without LUT-tables scheme.

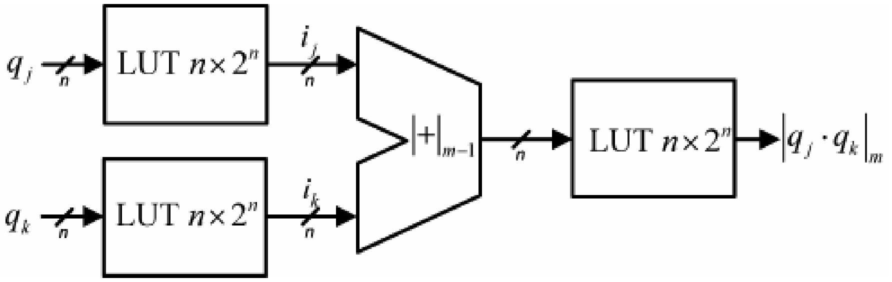

Fig. 4. Galois multiplier scheme.

Due to natural parallelism of residual classes system computations, it is reasonable to use the vector processors as a hardware platform. One of the most efficient models implementing a vector architecture is the product of Russian scientific and technical center “Module" - NM6403 processor. One of the most important features of NM6403 is working with operands of arbitrary length (even not divisible by a power of 2) in the range of 1-64 bits. This ensures the optimal balance between speed and accuracy of performing calculations. The ability to dynamically change the operands capacity can significantly increase overall productivity.

Besides NM6403 processors it is proposed to use a computing cluster of SISD architecture machines. Figure 5 provides an outline of the cluster, built at our university.

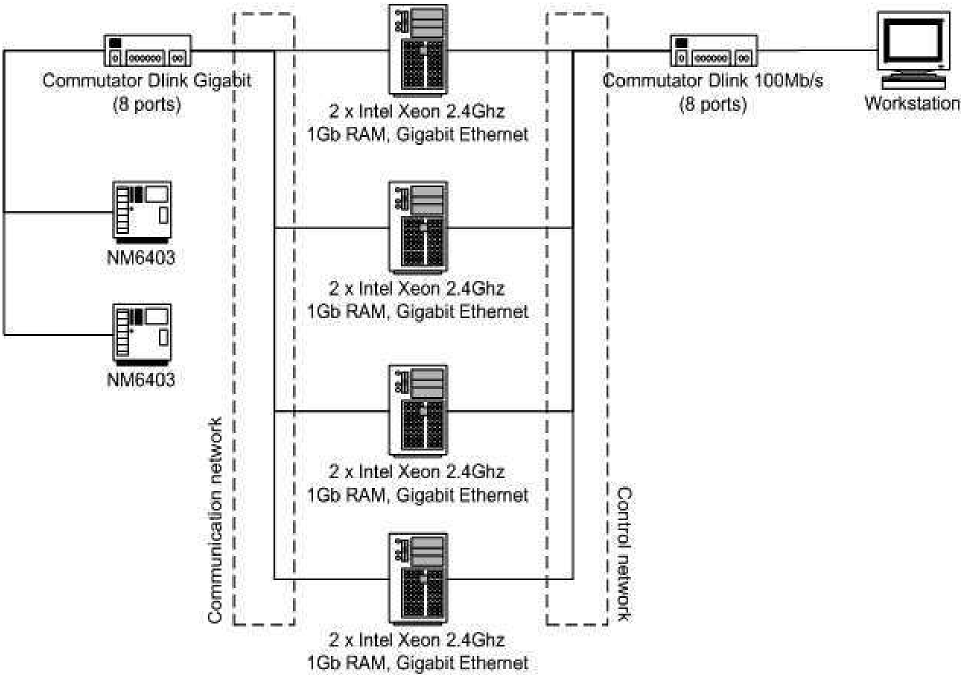

Fig. 5. Computing cluster scheme.

REFERENCES

1. Chervyakov, N.I., Dyachenko I.V. 2005. Designing modular adders and multipliers in *Proceedings of International Scientific Conference of Modular Arithmetic 2005*, Zelenograd, Russia.
2. Fomin, A.D. and Fomina A.V. 2004. Keys management in ad hoc networks. In *Proceedings of XII International New Informational Technologies Conference,* Moscow, Russia.
3. Tormasov, A.G., Hasin, M.A., Pahomov U.I. 2001. Distributed data storage system with controlled redundancy. *Researched in Russia 355*.

Oxana Mezentseva, North-Caucasus State Technical University
Aleksandr Alekseev, North-Caucasus State Technical University
Authors' addresses: Oxana Mezentseva, Department of Informational Technologies, North-Caucasus State Technical University, 355029, Russia; Alexander Alekseev, Department of Informational Technologies, North-Caucasus State Technical University, 355029, Russia.

Received September 2007